Patch Release Note

Patch 86231-09 For Rapier Switches and AR800 Series Modular Switching Routers

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86231-09 for Software Release 2.3.1 on existing models of Rapier L3 managed switches and AR800 Series L3 modular switching routers. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86231-09.

Base Software Release File	86s-231.rez
Patch Release Date	24-Dec-2002
Compressed Patch File Name	86231-09.paz
Compressed Patch File Size	906911 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.3.1 for Rapier Switches, AR300 and AR700 Series Routers, and AR800 Series Modular Switching Routers (Document Number C613-10325-00 Rev B) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.3.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Features in 86231-09

Patch 86231-09 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 02023 Module: PIM, VLAN Network affecting: No

When a VLAN port's layout changed, PIM was not updating correctly. Now PIM correctly updates a VLAN port's interface, neighbour and routes.

PCR: 02171 Module: STP, SWITCH, VLAN Network affecting: No

STP now operates on ports within a trunk group.

PCR: 02241 Module: FIREWALL Network affecting: No

Firewall subnet NAT rules were not working correctly from the private to the public side of the firewall. Traffic from the public to private side (destined for subnet NAT) was discarded. These issues have been resolved. ICMP traffic no longer causes a RADIUS lookup for access authentication, but is now checked by ICMP handlers for attacks and eligibility. If the ICMP traffic matches a NAT rule, NAT will occur on inbound and outbound traffic. HTTP 1.0 requests sometimes caused the firewall HTTP proxy to close prematurely. Cached TCP sessions were sometimes not hit correctly. These issues have been resolved.

PCR: 02300 Module: Firewall Network affecting: No

If the command ADD FIREWALL POLICY RULE SOURCEPORT=ALL was executed, a value of "65535" was incorrectly displayed for the SOURCEPORT parameter for that rule in the SHOW FIREWALL POLICY command. This issue has been resolved.

PCR: 02376 Module: PPP Network affecting: No

When the PPP ONLINELIMIT was exceeded for PPP over TDM, the PPP link stayed open, allowing Link Quality Report (LQR) packets to be transmitted. This caused the *ifOutOctets* counter to increment. Now, if the ONLINELIMIT is exceeded, the link will close.

PCR: 02395 Module: VRRP, TRG Network affecting: No

The SHOW VRRP command now shows the number of trigger activations for the Upmaster and Downmaster triggers.

PCR: 02396 Module: DHCP Network affecting: No

DHCP RENEW request messages are now unicast (as defined in the RFC), not broadcast.

PCR: 02400 Module: CORE,FFS,FILE,INSTALL,SCR Network affecting: No

If a problem occurred with NVS, some critical files were lost. As a result, the equipment was forced to load only boot ROM software at boot time. This patch combined with the new version of the boot ROM software (pr1-1.2.0 for the AR700 series) resolves this issue.

PCR 02408 Module: SWI Network affecting: No

The EPORT parameter in the SHOW SWITCH L3FILTER ENTRY command was displaying incorrectly after an issue was resolved in PCR02374. The command now displays correctly.

PCR: 02427 Module: DHCP Network affecting: No

DHCP entry reclaim checks are now delayed by 10 seconds if the entry is unroutable because the interface is not up.

PCR: 02463 Module: DVMRP, IPG Network affecting: No

Support for multi-homed interfaces has been added.

PCR 02465 Module: TTY Network affecting: No

Under some circumstances a fatal error occurred if a large amount of data was pasted onto the command line. This issue has been resolved.

PCR: 02489 Module: SWI Network affecting: No

When the switch was under heavy learning load, some MAC address were lost. This issue has been resolved.

PCR: 02499 Module: IPG Network affecting: No

Some parameters in the SET IP IGMP command had incorrect ranges. This issue has been resolved. The correct ranges are:

```
SET IP IGMP [LMQI=1..255] [LMQC=1..5]
   [QUERYINTERVAL=1..65535] [QUERYRESPONSEINTERVAL=1..255]
   [ROBUSTNESS=1..5] [TIMEOUT=1..65535]
```

PCR: 02506 Module: OSPF IPG Network affecting: No

The ADD IP ROUTE FILTER optional parameter INTERFACE caused the filter to not work on the OSPF external lsas' flooding.

The SHOW IP ROUTE FILTER interface name output was truncated to 6 characters. These issues have been resolved.

PCR: 02509 Module: DVMRP Network affecting: No

The source net mask has been removed from DVMRP *prune*, *graft* and *graft-ack* messages.

PCR: 02526 Module: DVMRP Network affecting: No

Under some circumstances, multiple default routes were created for DVMRP. This issue has been resolved.

PCR: 02532 Module: FIREWALL Network affecting: No

The Firewall showed the wrong counters on Total Received Packets and Dropped Packets and displayed twice the number of received packets when discarding packets from the public side. Also, when a Deny rule was applied to the private side, the Number of Dropped Packets was always zero. These issues have been resolved.

PCR: 02537 Module: L2TP Network affecting: No

When PPP was used over an L2TP tunnel, a speed of zero was shown for the PPP interface on the LNS side, while the LAC side showed a non-zero PPP interface speed. This issue has been resolved so that the LNS side of the PPP interface shows the correct speed.

PCR: 02538 Module: DVMRP Network affecting: No

The source mask is now always 0xffffffff in the DVMRP forwarding table.

The temporary route in the DVMRP route table was not displaying correctly. This issue has been resolved.

An IGMP entry was erroneously added for the reserved IP address. This issue has been resolved.

PCR: 02545 Module: IPG Network affecting: No

Previously, it was possible to add up to 33 IP interfaces. The correct limit is 32 IP interfaces. This issue has been resolved.

PCR: 02547 Module: IPG Network affecting: No

The ARP transmit counter total was not being incremented. This issue has been resolved.

PCR: 02552 Module: SWI Network affecting: No

If ingress filtering was supported within trunk groups, ports with ingress filtering enabled were erroneously added to the trunk group. This issue has been resolved.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

Features in 86231-08

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86231-08.

Base Software Release File	86s-231.rez
Patch Release Date	11-Oct-2002
Compressed Patch File Name	86231-08.paz
Compressed Patch File Size	371680 bytes

Patch 86231-08 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 02236 Module: FIREWALL Network affecting: No

Sometimes the retransmission of an FTP packet was not permitted through the Firewall. This issue has been resolved.

PCR: 02324 Module: SWI Network affecting: No

It is now possible to create 16 Layer 3 filters on Rapier *i* Series switches.

PCR: 02327 Module: IPG/FIREWALL Network affecting: No

In some situations, multihomed interfaces caused the Firewall to apply NAT and rules incorrectly when packets were received from a subnet that was not attached to the receiving interface. This issue has been resolved.

PCR: 02329 Module: DHCP Network affecting: No

An ARP entry for a host has been removed whenever a DHCP DISCOVER or DHCP REQUEST message is received from the host. This allows for clients changing ports on a switch.

PCR: 02332 Module: IPSEC Network affecting: No

The sequence number extracted from the AH and ESP header was in the wrong endian mode, which caused an FTP error with IPSEC anti-replay. This issue has been resolved.

PCR: 02340 Module: IPG Network affecting: No

If PIM is enabled, and the RESET IP INTERFACE command is executed, PIM is disabled. PIM now restarts automatically if this happens.

PCR: 02343 Module: PPP Network affecting: No

When acting as a PPPoE Access Concentrator (AC), if a PPPoE client sent discovery packets without the "host-unique" tag, the discovery packets sent by the AC were corrupted. This issue has been resolved.

PCR: 02359 Module: IPG Network affecting: No

When an IP Multihomed interface was used as an OSPF interface, neighbour relationships were only established if the IP interface for OSPF was added first in the configuration. Now, OSPF establishes neighbour relationships regardless of the IP Multihomed interface configuration order.

PCR: 02360 Module: DHCP Network affecting: No

This patch implements simple DHCP range MIBs, *dhcpRangeExhaustedGateway* and *dhcpRangeExhaustedInterface*, and a trap that shows when a DHCP range was exhausted. The trap is triggered when a DHCP request cannot be satisfied. The gateway address and the interface address are returned as trap variables.

PCR: 02362 Module: PIM Network affecting: No

If the HELLOINTERVAL parameter in the SET PIM command was less than 4 seconds, the PIM neighbour would time out. The minimum HELLOINTERVAL has been changed to 10 seconds for this command. Also, the commands SET IP INTERFACE and SET PIM INTERFACE were not recognising a modified IP address. The RESET PIM INTERFACE=VLAN command was not working correctly. These issues have been resolved.

PCR: 02364 Module: FFS Network affecting: No

The Flash compaction message has been changed from:
Flash compacting...
DO NOT restart the router until compaction is completed

To:
Flash compacting...
DO NOT restart the router, or power down until compaction is completed

PCR: 02365 Module: SWI Network affecting: No

Address learning on the mirror port is now correctly re-enabled when it is restored to its normal state.

PCR: 02366 Module: SWI Network affecting: No

If a gigabit fibre uplink was installed in a Rapier 24*i* or Rapier 48*i*, and the receive fibre was slowly withdrawn while the uplink was receiving heavy traffic, the switch chip sometimes locked up. This patch implements a workaround by causing a warm restart if this situation arises. A message is then written to the log to explain the cause of the restart.

PCR: 02368 Module: IPG/IGMP Network affecting: No

IGMP failed to create an automatic IGMP membership with no joining port when it received multicast data that no ports were interested in, when IP *TimeToLive* was set to 1 second. Also, IGMP erroneously sent a query on an IGMP enabled IP interface even when IGMP was disabled. These issues have been resolved.

PCR: 02374 Module: SWI Network affecting: No

In the ADD SWITCH L3FILTER command, the EPORT parameter incorrectly accepted the value 62-63 as multicast and broadcast ports 63-64. This issue has been resolved.

PCR: 02397 Module: DVMRP Network affecting: No

After a prune lifetime had expired, the interface was not joined back to the DVMRP multicast delivery tree. This issue has been resolved.

Features in 86231-07

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch 86231-07.

Base Software Release File	86s-231.rez
Patch Release Date	6-Sep-2002
Compressed Patch File Name	86231-07.paz
Compressed Patch File Size	355652 bytes

Patch 86231-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 01285 Module: OSPF Network affecting: No

When an interface went down (or was disabled) on an AS border router, the external routes were not removed from the routing domain. Such routes are now removed by premature aging.

PCR: 02003 Module: FIREWALL Network affecting: No

The timeout value for ICMP session entries in the firewall can now be adjusted via the OTHERTIMEOUT parameter of the SET FIRE POLICY command. Note: if the value for OTHERTIMEOUT is set to more than 10 minutes the timeout used for ICMP sessions will default to 10 minutes.

PCR: 02032 Module: VLAN Network affecting: No

An additional enhancement has been added for this previously released PCR. Now *ifOutOctets* increments correctly in the VLAN interface MIB.

PCR: 02036 Module: SWITCH Network affecting: No

A new command allows the Layer 3 aging timer to be changed:

SET SWITCH L3AGEINGTIMER=<seconds>

where seconds can be 30 - 43200. After each cycle of the ageing timer, all existing Layer 3 entries with the hit bit set will have the hit bit reset to zero, and all existing Layer 3 entries with the hit bit set to zero will be deleted.

The SHOW SWITCH command output now displays the Layer 3 ageing timer value.

PCR: 02083 Module: OGM/GUI Network affecting: No

The following additional enhancements have been added to this previously released PCR:

- The Set STP page now correctly displays the Bridge Priority, and not the root.
- The Priority field in the Add STP and Set STP pages now accepts five characters instead of four.
- The STP Monitoring page now displays the correct ports in the STP.
- The STP pages now lock correctly when no ports are selected.

PCR: 02102 Module: DVMRP Network affecting: No

DVMRP hold-down routing was not working correctly. This issue has been resolved.

PCR: 02111 Module: BGP Network affecting: No

Executing the RESET IP command left BGP peers in the DISABLED state. BGP was not aware when an IP interface changed state and consequently BGP got out of syncronisation with IPG. Multiple IP Routemap entries failed if the first entry had a different match type to the following entries. BGP peer update transmission was not operating correctly. A BGP peer that was in the ESTABLISHED state would still try to make TCP connections to its peer. These issues have been resolved.

PCR: 02128 Module: FIREWALL Network affecting: No

Some FTP packets handled by the firewall were forwarded with incorrect sequence numbers, causing FTP sessions to fail. This issue has been resolved.

PCR: 02150 Module: CORE, SNMP Network affecting: No

When passing 64-bit counters in an SNMP packet, only the lower 32 bits were passed. Now the full 64 bits of the counter will be returned if all are required.

PCR 02151 Module: IPG Network affecting: No

The Rapier was not detecting invalid checksums in ICMP echo request packets. This issue has been resolved. ICMP echo request packets with invalid checksums are now dropped and the ICMP *inErrors* and *inDiscards* counters are incremented.

PCR: 02167 Module: FIREWALL Network affecting: No

Locally generated ICMP messages, that were passed out through a firewall interface because they were associated with another packet flow, had their source address changed to that of the associated packet flow and were also forwarded with incorrect IP checksums. This only occurred when there was no NAT associated with the packet flow. This issue has been resolved.

PCR 02172 Module: IPG Network affecting: No

The TOS field in IP packets was not being processed by IP POLICY filters with an identifier greater than 7. This issue has been resolved.

PCR: 02174 Module: FIREWALL Network affecting: No

A feature has been added that makes pings pass from the source IP address of the public interface to the IP address on the private interface in the firewall.

PCR 02176 Module: FIREWALL Network affecting: No

Packets traversing in and out of the same public firewall interface were sometimes blocked. The firewall should only control packets passing between a public and a private interface. This issue has been resolved.

PCR 02178 Module: HTTP Network affecting: No

A buffer leak was associated with the HTTP server. This issue has been resolved.

PCR 02180 Module: IPG Network affecting: No

Multicast counters were not incrementing correctly. This issue has been resolved.

PCR 02184 Module: FFS FILE TTY Network affecting: No

This patch supersedes PCRs 02073, 02081, 02086 and 02105. In addition to enhancements in the preceding PCRs, this PCR now also resolves the following issues:

- If a compaction was started within 60ms of a file write commencing, the file being written was placed in the wrong location in the file system. This led to file corruption during subsequent compactions.
- If a file load occurred during compaction, an incomplete copy of the file was loaded. The load also put the file into the wrong part of the file system once the compaction had moved beyond the part of the file that had been loaded.
- A fatal error occurred during compaction if a file was marked as deleted when it was being transferred.

- Sometimes during compaction when the file system was erasing blocks belonging to deleted files, one of the files was transferred rather than deleted. However, its directory entry was deleted, so the file was not visible with a SHOW FILE command but was visible with a SHOW FFILE command.
- During compaction if the amount of free space was less than two erase blocks (including the "spare" erase block), the file system erroneously reported that a large amount of space was available for a new file due to an underflow problem. When a new file was written it would corrupt existing data.
- If the file system was completely full and the deletion of a single file led to a compaction, the file system reported that it was continually compacting. This was because it was repeatedly searching through a linked list of file headers.
- A byte of data from FLASH was incorrectly returning the value 0xFF.
- When a file was renamed using upper case letters, the renamed file did not appear in the file directory but did appear in FLASH. Also, if a SHOW FFILE CHECK command was executed after renaming the file, the file system would appear to hang. All file names must now be lower case.
- Multiple TTY sessions could edit the same file. This caused unpredictable behaviour when the TTY sessions closed the files.

A new command, SHOW FFILE VERIFY, has been added. This command steps through the file system headers starting with file zero and finishing at the end of the last reachable file. It then verifies that all FLASH locations from the end of the last reachable file to the beginning of file zero are in an erased state. Errors are reported as they are found.

PCR: 02185 Module: VRRP Network affecting: No

The SHOW CONFIG DYNAMIC=VRRP command was not showing port monitoring and step values correctly. This issue has been resolved.

PCR 02188 Module: VRRP Network affecting: No

When VRRP responded to an ARP request for the VR IP address it was not making an entry in the ARP table and the switch L3 table. This issue has been resolved.

PCR 02194 Module: SWI Network affecting: No

Untagged Layer 2 packets selected for mirroring were incorrectly transmitted from the mirror port with a tag. This issue has been resolved.

PCR: 02195 Module: SWI Network affecting: No

If a port on a Rapier 48 or Rapier 48*i* went down, some associated entries were not promptly removed from the forwarding, Layer 3 and default IP tables. This issue has been resolved.

PCR: 02198 Module: DHCP Network affecting: Yes

This PCR includes the following enhancements:

- A new command, SET DHCP EXTENDID allows for multiple DHCP clients, and handling of arbitrary client IDs on the server.
- Static DHCP entries now return to the correct state when timing out.
- DHCP entry hashes now have memory protection to prevent fatal errors.

- DHCP client now retransmits XID correctly.
- Lost OFFER messages on the server are now handled correctly.

The DHCP server now correctly handles DHCP clients being moved to a different interface on the DHCP server after they've been allocated an IP address.

PCR: 02199 Module: TRIGGER Network affecting: No

The CPU and MEMORY parameters in the SET TRIGGER command erroneously accepted the minimum value "0" rather than "1". This issue has been resolved.

PCR: 02202 Module: FIREWALL/IP NAT Network affecting: No

Previously, when Firewall or IP NAT was enabled, any fragmented IP packets had to be reassembled so they could be processed. If the fragments could not be reassembled, the packet was dropped. Reassembly could only occur if the combined packet (IP header, and protocol header, and data) was no more than 1800 bytes. An additional limit of no more than eight fragments was also imposed. This PCR implements enhanced fragment handling for Firewall and IP NAT. Each module can now be configured to process fragmented packets of specified protocol types without needing to reassemble the packet. The number of fragments a packet may consist of is also configurable. This enhanced fragment handling is disabled by default.

To enable enhanced fragmentation for Firewall, use the command:

```
ENABLE FIREWALL POLICY=policy_name
   FRAGMENT={ICMP|UDP|OTHER}
```

To enable enhanced fragmentation for IP NAT, use the command:

```
ENABLE IP NAT FRAGMENT={ICMP|UDP|OTHER}
```

To disable enhanced fragmentation for Firewall, use the command:

```
DISABLE FIREWALL POLICY=policy_name
   FRAGMENT={ICMP|UDP|OTHER}
```

To disable enhanced fragmentation for IP NAT, use the command

```
DISABLE IP NAT FRAGMENT={ICMP|UDP|OTHER}
```

To configure the number of fragments permitted per packet for Firewall, use the command:

```
SET FIREWALL FRAGMENT=8...50
```

To configure the number of fragments permitted per packet for IP NAT, use the command:

```
SET IP NAT FRAGMENT=8...50
```

TCP has been excluded from this enhancement because TCP has the MSS (Maximum Segment Size) parameter for segment size control. Also, for PPPoE interfaces with a reduced MTU of 1492, a previous enhancement in PCR 02097 ensures that TCP MSS values in sessions carried by a PPPoE interface are clamped to a value that prevents fragmentation.

PCR: 02214 Module: IPG Network affecting: No

A buffer leak occurred when a large number of flows (over 4000) were in use and needed to be recycled. This issue has been resolved.

PCR: 02215 Module: FILE Network affecting: No

When the only feature licence in the feature licence file was disabled, the licence file stored on FLASH memory did not change. This was due to a previous enhancement in PCR 02184 which prevented existing files being deleted before a new version was stored. This issue has been resolved.

PCR 02217 Module: OSPF Network affecting: No

A restriction now applies to the generation of unnecessary OSPF indication LSAs, originated when a neighbour router does not support OSPF demand circuits.

PCR: 02220 Module: SWI Network affecting: No

The EPORT parameter in the ADD SWITCH L3FILTER ENTRY and SET SWITCH L3FILTER ENTRY commands was matching multicast and broadcast packets with software filtering. This issue has been resolved.

PCR 02222 Module: IPG Network affecting: No

Packets were incorrectly being switched by hardware when filters were enabled. Packets are now switched in software if filters are set, and are switched in hardware if no filters are set.

PCR: 02229 Module: IPG Network affecting: No

The PURGE IP command now resets the IP route cache counters to zero.

PCR: 02240 Module: SWI Network affecting: No

The SENDCOS filter action did not operate correctly across switch instances. This was because the stacklink port on the Rapier 48 did not correctly compensate for the stack tag on frames received via the filter. This issue has been resolved.

PCR: 02242 Module: IPG Network affecting: No

On a Rapier 24, adding an IP interface over a FR interface caused an ASSERT debug fatal error. This issue has been resolved.

PCR 02244 Module: UTILITY Network affecting: No

Virtual interfaces were displayed incorrectly when VLANs were multihomed. This issue has been resolved.

PCR: 02245 Module: VRRP Network affecting: No

VRRP returned an incorrect MAC address for an ARP request. This issue has been resolved.

PCR 02248 Module: IPSEC, IPG Network affecting: No

Fragmented packets with a total length greater than 1800 bytes are handled using chained packets. IPSEC does not process chained packets and was discarding them even if the IPSEC policy action was set to PERMIT. This enhancement allows fragmented packets greater than 1800 bytes to be passed by the switch when IPSEC is enabled and the action is set to PERMIT.

PCR: 02250 Module: FIREWALL Network affecting: No

Sometimes the Firewall erroneously used NAT. This issue has been resolved.

PCR 02257 Module: SWI/VLAN Network affecting: No

An IGMP multicast storm sometimes occurred on trunked ports. This issue has been resolved.

PCR: 02259 Module: DHCP, IPG Network affecting: No

A dual Ethernet router was incorrectly accepting an IP address from a DHCP server when the offered address was on the same network as the other Ethernet interface. An error is now recorded when DHCP offers an address that is in the same subnet as another interface.

PCR: 02260 Module: TTY Network affecting: No

When a '\n'(LF) character was received, the router/switch did not recognise this as the termination of a command over Telnet. This issue has been resolved.

PCR: 02262 Module: DNS Network affecting: No

Responses to MX record requests were not handled correctly if the preferred name in the MX record differed from the one that was requested. This issue has been resolved.

PCR: 02263 Module: VRRP Network affecting: No

The virtual MAC address was used as the source MAC for all packets forwarded on an interface associated with a Virtual Router (VR). This was confusing when multiple VRs were defined over the same interface because only one virtual MAC address was ever used. The other virtual MAC addresses (for the other VR's) were only used if the source IP address matched the VR's IP address. To avoid this confusion, the system MAC address is now always used unless the source IP address of the packet is the same as the VR's IP address.

PCR: 02264 Module: PIM, DVMRP, SWI Network affecting: No

PIM or DVMRP failed to see any data if IGMP snooping was on and DVMRP or PIM was enabled after the data stream had reached the router/switch. This issue has been resolved.

PCR: 02268 Module: FIREWALL Network affecting: No

HTTP requests from a fixed IP address were erroneously reported as a host scan attack in the Firewall deny queue. This issue has been resolved.

PCR: 02274 Module: TPAD Network affecting: No

ARL message interrupts have been re-enabled after a software table rebuild to fix synchronisation of the software forwarding database with the hardware table.

PCR: 02275 Module: OSPF Network affecting: No

Some routes were not added into the OSPF route list, and therefore were not added into the IP route table. This issue has been resolved.

PCR: 02276 Module: FIREWALL Network affecting: No

The CREATE CONFIG command did not save the SOURCEPORT parameter to the configuration file when the low value of the source port range was set to zero. This issue has been resolved.

PCR: 02287 Module: IPG Network affecting: No

Existing IGMP groups were not deleted when IGMP was disabled globally or on the associated interface. This gave the groups very high timeout values. This issue has been resolved.

PCR: 02292 Module: IPSEC Network affecting: No

IPSec no longer logs packets that match an ACTION=ALLOW policy. The overhead of this logging was affecting non-IPSec traffic.

PCR: 02293 Module: ENCO Network affecting: No

The ENCO key creation thread did not suspend to allow other processes any CPU time. This caused the command prompt to freeze during key creation. This issue has been resolved.

PCR: 02294 Module: IKMP Network affecting: No

The LOCALRSAKEY parameter in the CREATE ISAKMP POLICY and SET ISAKMP POLICY commands was not accepting the value zero. This issue has been resolved.

PCR: 02299 Module: VRRP Network affecting: No

If a packet with a destination IP address equal to a VRRP IP address was received when the router didn't own the IP address, (because it didn't have an interface with that IP address) the router incorrectly tried to forward the packet and send an ICMP "redirect" message to the source. Now, if such a packet is received, it will be discarded and an ICMP "host unreachable" message will be sent to the source.

PCR: 02301 Module: IPG Network affecting: No

If a DNS relay agent was configured with overlapping subnets, sometimes the DNS server response was returned to the client with a source IP address of an interface of the relay agent that was different from the interface the request was received on. This issue has been resolved.

PCR: 02303 Module: INSTALL Network affecting: No

When enabling or disabling feature licences, a message will now be generated with a warning that changes to feature licences may not take effect until after a reboot.

PCR: 02304 Module: VRRP Network affecting: No

VRRP used the wrong source IP address in ICMP redirects. RFC 2338 states that the source IP address of ICMP redirects should be the IP address that the end host used when making its next hop routing decision. In the case of a packet sent to a VRRP virtual MAC address, this is the primary VRRP IP address associated with the MAC address, provided such a VR exists and is in the master state. This issue has been resolved.

PCR: 02305 Module: STP, VLAN Network affecting: No

If IGMP and STP were enabled, and an IGMP packet was received on a STP blocking port, the packet was forwarded to another port, causing an IGMP storm. This issue has been resolved.

PCR: 02308 Module: SWI Network affecting: No

This PCR implements fan threshold control, parity enable/disable, A39 link card enable/disable and Cell Buffer Pool Global Buffer Pool (CBPGBP) enable/disable.

PCR: 02316 Module: CORE Network affecting: No

Some board names for the Rapier 24*i* and Rapier 48*i* were incorrect. This issue has been resolved.

PCR: 02317 Module: IPG Network affecting: No

The SIZE functionality on the IP filter was not working for IP fragmented packets. This issue has been resolved.

PCR: 02319 Module: DHCP Network affecting: No

DHCP requests for IP addresses on incorrect and unroutable subnets would fail. The DHCP server now offers an IP address on a valid subnet.

PCR: 02323 Module: SWI Network affecting: No

Layer 3 switch load balancing has been implemented across trunked ports.

Features in 86231-06

Patch file details are listed in Table 4:

Table 4: Patch file details for Patch 86231-06.

Base Software Release File	86s-231.rez
Patch Release Date	17-May-2002
Compressed Patch File Name	86231-06.paz
Compressed Patch File Size	199360 bytes

Patch 86231-06 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 01200 Module: OSPF Network affecting: No

OSPF has been modified to utilise a 0.1s tick, as opposed to a 20ms tick.

PCR 01239 Module: IKMP, IPG Network affecting: Yes

IKE failed to negotiate with a peer when the negotiation was triggered by the PRENEGOTIATE parameter of the CREATE ISAKMP POLICY and SET ISAKMP POLICY commands. This issue has been resolved.

PCR: 01241 Module: OSPF, IPG Network affecting: No

OSPF performance has been improved by running it as a separate thread.

PCR: 01242 Module: CORE, SNMP Network affecting: No

The switch now delays sending link traps immediately after a restart to give the link to the trap host time to come up. A similar change has been made for the cold start trap. After a 10s delay, all interfaces which are UP have a link trap generated for them. After that, link traps are sent as normal.

PCR: 01287 Module: OSPF, IPG Network affecting: No

Configuring IP route filters did not stop flooding of AS external LSAs to neigbours at startup. The result was that the neigbour received the AS LSAs and added the corresponding routes into its own routing table. However, after some time (e.g. 1 hour), the AS external LSAs in the neigbour's database disappeared, but the corresponding routes were still in its routing table. This issue has been resolved.

PCR: 02073 Module: FILE Network affecting: No

If a flash write error occurred when a file was being written, the file's directory entry was deleted leaving a partial file in flash. Subsequent attempts to write the file failed because a file of the same name already existed. This issue has been resolved.

PCR: 02075 Module: OSPF, IPG Network affecting: No

In configurations containing a large number of OSPF routes, the SPF calculation could take a long time. During this calculation, other events would not be processed. This patch reduces the time required for an SPF calculation and allows the switch to respond to other events in the mean time. This patch also improves the performance of flow cache updates.

PCR: 02081 Module: FILE, FFS Network affecting: No

If the FILE module was required to re-write a file, the existing file would be deleted before the size of the new file was known. This issue has been resolved.

PCR: 02083 Module: IPG Network affecting: No

The following issues have been resolved:

- The GUI suffered a fatal error when multiple users browsed to single-user pages.
- It was not possible to modify port settings.
- "Enable" and "disable" GUI handlers were not working correctly.
- Incorrect commands were not dealt with correctly, locking the GUI.
- The layer 3 "modify" buttons were not working correctly.
- "Remove" buttons attempted to operate if no selection was made.
- "Modify" pages did not show any data.

Also, support has been added for the Rapier 16i, 24i and 48i models.

PCR: 02083 Module: HTTP Network affecting: No

The GUI stopped working when a VLAN's IP address was changed. This issue has been resolved.

PCR: 02083 Module: SWI Network affecting: No

The formatting of the GUI-FIELD-LEARNED field for the 0 learned case has been improved.

PCR: 02083 Module: CORE Network affecting: No

Long system location strings now operate correctly. Also, support has been added for A40 and A42 uplink cards.

PCR: 02086 Module: FFS Network affecting: No

If a file ended short of an erase block boundary and a compaction was started, the block in which the file was stored was not erased, causing errors when new files were written. Also, if the last file in the filing system ended on or short of an erase block boundary, and a compaction was started, then compaction would fail. These issues have been resolved.

PCR: 02105 Module: FFS Network affecting: No

An error occurred when the FLASH write driver was required to write values that were not long-word aligned and were at the driver's page boundary. The driver attempted to write into the next section of memory. It also attempted to read the status of this section of memory, and misinterpreted the result as a low Vpp voltage. Also, errors occurred during FLASH compaction. These issues have been resolved.

PCR: 02113 Module: SWI Network affecting: No

When a Rapier with C revision silicon received a multicast packet, the ifOutError port counter was incorrectly incremented. This issue has been resolved.

PCR: 02116 Module: IPG PING Network affecting: No

When pinging to a remote IP address with two or more different cost routes, if the preferred route became unavailable, the ping failed to switch to the less preferred route until the ping was stopped and restarted. This issue has been resolved.

PCR: 02118 Module: SWI Network affecting: No

When the command SH SWI PORT ? was entered, the parameter options VLAN and SOCK were displayed. They should not have been because they are not valid parameters for the command. Executing the command with the SOCK parameter caused a fatal error. These issues have been resolved.

PCR: 02120 Module: IPG Network affecting: No

When a Rapier was restarted the IP address of the domain name server was not displayed on the IP General GUI page. This issue has been resolved.

PCR: 02121 Module: SWI Network affecting: No

When an STP instance was enabled for the first time on a Rapier 48, BPDU transmission on ports 25-48 was delayed for up to 30 seconds. STP BPDUs are now transmitted as soon as the STP instance is enabled.

PCR: 02123 Module: IPG Network affecting: No

The IP, MASK, and ACTION parameters could not be set with the SET IP ROUTE FILTER command. This issue is resolved when the filter number is specified at the start of the command, for example:

```
SET IP ROUTE FILTER=filter-id IP=ipadd MASK=ipadd
ACTION={INCLUDE|EXCLUDE}
```

where: *filter-id* is the filter number. Filter numbers are displayed in the output of the SHOW IP ROUTE FILTER command.

PCR: 02130 Module: SWI Network affecting: No

A port that was deleted from a VLAN continued to switch packets, and entries remained in the ARP and LAYER 3 hardware tables when they should have been removed. These issues has been resolved.

PCR 02135 Module: SSH Network affecting: No

Logging out of a Secure Shell session sometimes caused a restart. This issue has been resolved.

PCR 02136 Module: FIREWALL Network affecting: No

The firewall was blocking outbound ICMP packets when the associated private interface had a 'deny all' rule. The forwarding of packets is now controlled by the ICMP_FORWARDING and PING parameters.

PCR 02137 Module: ISAKMP Network affecting: No

The ISAKMP main and aggressive exchanges could get stuck in the KE sent state if an SA message was received from the remote device when a KE message was expected. This issue has been resolved.

PCR 02138 Module: SWI Network affecting: No

The built in Self Test Code for all Rapiers, except G6, has been improved to enhance the detection of faults in switch chip external packet memory.

PCR 02142 Module: ISAKMP Network affecting: No

The enco key disappeared from the flash after reboot. This issue has been resolved.

PCR 02144 Module: IPG Network affecting: No

The IPG module has been enhanced to support gratuitous ARP request and ARP reply packets.

PCR 02145 Module: IPG Network affecting: No

The IGMP refresh timer could incorrectly be show a value greater than 4000000000. This issue has been resolved.

PCR 02146 Module: SWI Network affecting: No

The Layer 3 filter was not working on ports 25-48 if the ingress port was different from the egress port. This issue has been resolved.

PCR 02147 Module: SWITCH, VLAN Network affecting: No

If only one uplink card was present, and it was in the bottom bay of the Rapier, then the VLAN module would incorrectly register the presence of an uplink card in the top bay.

PCR 02148 Module: ISAKMP Network affecting: No

The CREATE CONFIG command no longer outputs the POLICYFILENAME parameter if the value has not been set.

PCR 02149 Module: TTY Network affecting: No

SSH clients were unable to logout and caused the system to freeze. Incorrect logins caused an infinite lockout. These issues have been resolved.

PCR 02151 Module: IPG Network affecting: No

The Rapier was not detecting invalid checksums in ICMP echo request packets. This issue has been resolved. ICMP echo request packets with invalid checksums are now dropped and the ICMP *inErrors* and *inDiscards* counters are incremented.

PCR 02153 Module: SWI Network affecting: No

The following issues have been resolved:

- If an A39 port was forced to a fixed 10Mbit or 100Mbit speed, then its configuration would become MDI when it should have been MDI-X.
- If an A39 port was set to operate in duplex mode, at 1000Mbit, the output of the SHOW CONFIG DYNAMIC command did not match the new settings.

.

PCR 02160 Module: PIM Network affecting: No

If PIM DM was configured with multicast switch emulation, and OSPF was configured and the switch was restarted during the processing of multicast packets, PIM DM was updated with the correct route information, however, the MARL table was updated with incorrect information. This caused packets to be forwarded by software instead of being switched by hardware, or dropped. This issue has been resolved.

PCR 02161 Module: IPG Network affecting: No

The IP Filter SIZE parameter was not being applied correctly. This issue has been resolved.

PCR 02162 Module: IPG Network affecting: No

The SET IP FILTER command would not update the SIZE parameter correctly. This issue has been resolved.

PCR 02165 Module: IPG Network affecting: No

If the IGMP query interval was set to less than 4 seconds, then IGMP query messages were not sent. This issue has been resolved.

PCR 02169 Module: IPG Network affecting: No

An issue with multicast code which is used for copying multicast packets has been resolved.

PCR 02175 Module: IPG Network affecting: No

Equal cost multipath routing sometimes failed to use equal cost routes in balance. This issue has been resolved.

Features in 86231-05

Patch file details are listed in Table 5.

Table 5: Patch file details for Patch 86231-05.

Base Software Release File	86s-231.rez
Patch Release Date	11-Apr-2002
Compressed Patch File Name	86231-05.paz
Compressed Patch File Size	140084 bytes

Patch 86231-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 01263 Module: FIREWALL Network affecting: No

The firewall TCP timeout values for sessions in the CLOSED and TIMEWAIT states have been reduced. This only applies to the stateful inspection of firewall sessions and not to the TCP module.

PCR: 01275 Module: FIREWALL Network affecting: No

The firewall was incorrectly forwarding multicast packets originating from a private address in cases where a matching route was defined. This issue has been resolved.

PCR: 02020 Module: SWI Network affecting: No

When disabling port mirroring the VLAN tagging configuration of other ports was corrupted. This issue has been resolved.

PCR: 02024 Module: IPG Network affecting: No

Proxy Arp can now be used on VLAN interfaces.

PCR: 02032 Module: SWI VLAN Network affecting: No

A protected VLAN feature has been added. This enables the network manager to prevent inter-port communication between devices connected to ports in the same VLAN.

PCR: 02041 Module: SWI Network affecting: No

In some situations, the switch would stop forwarding packets via internal and/or external uplink ports. This issue has been resolved.

PCR: 02051 Module: VRRP Network affecting: No

When using VRRP interface monitoring, but not port monitoring, the VRRP priority could be incorrect. Also, the dynamic priority value rather than the configured priority value was appearing in router generated configurations. These issues have been resolved.

PCR: 02052 Module: LOAD Network affecting: No

Uploading a file with TFTP that included a directory name (eg. tftptest/testfile.txt) caused a fatal error. This issue has been resolved. Also, the pathname length has been increased from 40 to 100 characters.

PCR: 02054 Module: SWI, CORE Network affecting: No

Support for the A42 GBIC uplink has been added.

PCR: 02057 Module: FIREWALL Network affecting: No

Firewall TCP timeout values have been reduced for sessions placed in the CLOSED state after receiving a TCP/RESET. This applies to the stateful inspection of firewall sessions only, and not to the TCP module. Previously, PCR 01263 reduced the timeout value for sessions placed in the CLOSED state after a TCP/FIN packet was received.

PCR: 02058 Module: CORE, SNMP Network affecting: No

An SNMP GET-NEXT request for *fanAndPsTemperatureStatus.0* returned an incorrect *noSuchName* error. Also, instance *restart.0* was unreachable because *restartMibTable* was not initialised correctly. These issues have been resolved.

PCR: 02062 Module: SWI Network affecting: No

The Gigabit Maximum frame length has been increased to 1528 bytes to allow passing of Stacking Link Port frames.

PCR: 02063 Module: FIREWALL Network affecting: No

Firewall IP access lists were not working correctly. If an IP range was specified without spaces between the IP address and the separating '-' the range would be ignored. Spaces are no longer required. Also, matches were made to addresses covered by a range in an access list if the matching range was numerically the lowest in the list. This issue has been resolved.

PCR: 02066 Module: STP Network affecting: No

After increasing the switch's STP priority, the Designated Root information was not updated. This issue has been resolved.

PCR: 02070 Module: CORE Network affecting: No

The TickTimer ran one percent slower than it should have. This issue has been resolved.

PCR: 02071 Module: NTP Network affecting: No

When a NTP packet was received from an NTP server (mode 4) the router acted as a client, and sent a reply back to the server, but did not remove the peer association. This meant that the Dynamic Peers list, viewed using the SHOW NTP command, displayed incorrect dynamic peer associations. This issue has been resolved.

PCR: 02076 Module: SWI, VLAN Network affecting: No

If ingress bandwidth limiting was set below 1000, ICMP (ping) packets were no longer passing through the switch. This issue has been resolved. Also, if packet debugging was enabled, and a packet received on a VLAN was for another VLAN, the packet was not displayed by debug before it was dropped. This issue has been resolved.

PCR: 02078 Module: IPG Network affecting: No

ARP was not completing when an interface was down. This issue has been resolved.

PCR: 02082 Module: OSPF Network affecting: Yes

OSPF virtual links running across a single network segment would accept 0.0.0.0 as the next hop address. This was inherited by derivative routes, making them unusable. This issue has been resolved.

PCR: 02083 Module: IPG Network affecting: No

The following issues have been resolved:

- The GUI suffered a fatal error when multiple users browsed to single-user pages.
- It was not possible to modify port settings.
- "Enable" and "disable" GUI handlers were not working correctly.
- Incorrect commands were not dealt with correctly, locking the GUI.
- The layer 3 "modify" buttons were not working correctly.
- "Remove" buttons attempted to operate if no selection was made.
- "Modify" pages did not show any data.

Also, support has been added for the Rapier 16i, 24i and 48i models.

PCR: 02083 Module: HTTP Network affecting: No

The GUI stopped working when a VLAN's IP address was changed. This issue has been resolved.

PCR: 02083 Module: SWI Network affecting: No

The formatting of the GUI-FIELD-LEARNED field for the 0 learned case has been improved.

PCR: 02083 Module: CORE Network affecting: No

Long system location strings now operate correctly. Also, support has been added for A40 and A42 uplink cards.

PCR: 02084 Module: FIREWALL Network affecting: No

Pings to the public interface of the firewall sometimes failed. This issue has been resolved.

PCR: 02085 Module: SWI Network affecting: No

The default route table (DEFIP table) could be corrupted when RIP routes were added or deleted from the table. This issue has been resolved.

PCR: 02089 Module: SWI Network affecting: No

The port number is now considered when the layer 3 routing table is displayed.

PCR: 02090 Module: SWI Network affecting: No

A fatal error occurred when default routes in the DEFIP table were associated with a port whose status changed (up/down). Also, invalid routes that were deleted from DEFIP were not re-added to DEFIP when they became valid again. These issues have been resolved.

PCR: 02092 Module: SWI Network affecting: No

The SET SWITCH L3 FILT command overwrote existing Layer 3 filters. If multiple filter entries existed, this command changed the most recent entry, rather than the one specified. These issues have been resolved. Also, the SET SWITCH L3 FILT command now allows for creation of multiple filter entries with the SETPRIORITY and SETTOS parameters. The Layer 3 filter protocol match now has no limit.

PCR: 02093 Module: SWI Network affecting: No

Improvements have been made to trunking on all Rapier models. Now the master (lead) port of the trunk group is always configured correctly.

PCR: 02094 Module: IPG Network affecting: No

When an IP flow table contained the IP flow structure for a spoofed packet, the SHOW IP FLOW command would crash when executed. This issue has been resolved.

PCR: 02095 Module: SWI Network affecting: No

The software routing performance of the Rapier 48 and Rapier 48i has been enhanced.

PCR: 02096 Module: IPG, SWI Network affecting: No

When the switch received an IGMP query, it created an entry in the hardware-based multicast table that had incorrect port tagging information. This issue has been resolved. Also, IGMP will no longer participate in changing the hardware multicast table when IP multicast switching emulation is enabled.

PCR: 02098 Module: STP Network affecting: No

STP always transmits untagged packets. If a port does not belong to a VLAN as an untagged port, then the port must belong to one VLAN as a tagged port. In this case, STP should transmit VLAN tagged packets out of the port.

PCR: 02099 Module: DHCP Network affecting: No

A switch sometimes restarted if it was configured with static DHCP entries and was handling a large number of DHCP clients. This issue has been resolved.

PCR: 02100 Module: PIM Network affecting: No

When a VLAN was configured as a PIM interface, and had trunked ports as members, PIM did not work properly on the trunked ports. This issue has been resolved.

PCR: 02101 Module: SWI Network affecting: No

The layer 3 hardware table was not sorted properly when it contained a very wide range of IP addresses (eg. 10.0.0.1 - 205.33.3.1). This caused a small number of packets to be routed by software rather than hardware. This issue has been resolved.

PCR: 02103 Module: SWI Network affecting: No

IPX traffic passing between two switch instances using VLAN for Rapier48 now operates correctly.

PCR: 02104 Module: TRG Network affecting: No

The periodic and time trigger counts were incrementing by two instead of one on each update. This issue has been resolved.

PCR: 02106 Module: IPG Network affecting: No

The ADD IP ARP command can now accept ports 49 and 50.

Features in 86231-04

Patch file details are listed in Table 6:

Table 6: Patch file details for Patch 86231-04.

Base Software Release File	86s-231.rez
Patch Release Date	27-Feb-2002
Compressed Patch File Name	86231-04.paz
Compressed Patch File Size	58456 bytes

Patch 86231-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 02005 Module: IPG Network affecting: No

When telnetting to the switch, the TCP connection was reset, and when the packet was passed to IPG_Forward a fatal error occurred. This patch implements a workaround.

PCR: 02056 Module: IGMP Network affecting: No

An addition to the patch resolves issues with IGMP reflooding query packets to tagged ports.

Features in 86231-03

Patch file details are listed in Table 7:

Table 7: Patch file details for Patch 86231-03.

Base Software Release File	86s-231.rez
Patch Release Date	21-Feb-2002
Compressed Patch File Name	86231-03.paz
Compressed Patch File Size	57516 bytes

Patch 86231-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 01288 Module: SWI Network affecting: No

In situations where a switch port has been forced to half duplex mode and the link partner is forced to full duplex mode it is possible for the switch to enter a state where it is unable to transmit packets. This patch prevents this state from being reached despite the misconfiguration.

PCR: 02019 Module: SWI Network affecting: No

If a layer 3 hardware filter for a particular packet type (e.g. Netbeui) was configured, all IP packets destined for the CPU were discarded. This issue has been resolved.

PCR: 02035 Module: VLAN Network affecting: No

The CREATE CONFIG command now correctly configures tagged ports belonging to VLANs not in the default STP.

PCR: 02042 Module: LPD Network affecting: No

The TCP port 00515 (LPD) is now closed by default until a CREATE LPD command is executed. The port then remains open until a router restart.

PCR: 02043 Module: X25 Network affecting: No

The X.25 TCP listen port (01998) is now closed by default until a CREATE X25C command or SET X25C TCPKEEPALIVE command is executed. The port then remains open until a router restart.

PCR: 02044 Module: STT Network affecting: No

The TCP listen port 05026 (STT) is now closed by default until a ADD STT command is executed. The port then remains open until a router restart.

PCR: 02045 Module: OGM Network affecting: No

Improved the display of buttons when using the Netscape browser, and improved the Modify VLAN page in the GUI.

PCR: 02047 Module: SWI Network affecting: No

Invalid values were presented when reading MIB variables from the STP port table. This issue has been resolved.

PCR: 02048 Module: CORE Network affecting: No

Some Rapier products returned invalid sysObjectIds. This issue has been resolved.

PCR: 02049 Module: IPG Network affecting: No

Special multicast packets (ie. 224.0.0.3 - 224.0.0.255) were sometimes not recognised as being multicast packets. This issue has been resolved.

PCR: 02050 Module: RMON Network affecting: No

Some SNMP trap identifiers generated by a rising or falling alarm were incorrect. This issue has been resolved.

PCR: 02056 Module: IGMP Network affecting: No

Incoming multicast traffic from a source connected to a switch port operating in multicast mode B (flood multicast packets with no registered member) will no longer flood the VLAN associated with the port. Only member ports and router ports on the same VLAN will receive the traffic.

Features in 86231-02

Patch file details are listed in Table 8.

Table 8: Patch file details for Patch 86231-02.

Base Software Release File	86s-231.rez
Patch Release Date	8-Feb-2002
Compressed Patch File Name	86231-02.paz
Compressed Patch File Size	40272 bytes

Patch 86231-02 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 02033 Module: SWI Network affecting: No

When a Rapier "i" series switch transmitted an internally generated tagged packet, the packet was transmitted with an FCS error. This issue has been resolved.

PCR: 02034 Module: SWI Network affecting: No

Under certain circumstances multicast packets were duplicated on egress. This issue has been resolved.

Features in 86231-01

Patch file details for Patch 86231-01 are listed in Table 9.

Table 9: Patch file details for Patch 86231-01.

Base Software Release File	86s-231.rez
Patch Release Date	5-Feb-2002
Compressed Patch File Name	86231-01.paz
Compressed Patch File Size	39804 bytes

Patch 86231-01 includes all issues resolved and enhancements released in previous patches for Software Release 2.3.1, and the following enhancements:

PCR: 01214 Module: SWI Network affecting: No

In a Rapier G6, fitted with a fibre uplink module with all ports active, switching traffic between port 1 and the uplink caused the traffic flow to cease after a period of time depending on the volume of traffic. This issue has been resolved.

PCR: 01221 Module: SWI Network affecting: No

Flow control performance has been improved.

PCR: 01243 Module: SWI Network affecting: No

When a Rapier CPU was handling a large amount of traffic and a busy egress port went down, it was possible for the transmission of packets by the CPU to cease. This issue has been resolved.

PCR: 01249 Module: CORE, SWI Network affecting: No

Support for the AT-40/41 100Mbit fibre uplink modules has been added.

PCR: 01250 Module: SWI Network affecting: No

On Rapier "i" series models, outgoing packets (originating from the CPU) consisting of chained buffers were corrupted by the insertion of four bytes at the end of the first buffer in the chain. This affected L2TP calls over an Ethernet connection. This issue has been resolved.

PCR: 01252 Module: SWI Network affecting: No

On the Rapier 48 in certain circumstances (e.g. a routing update or ARP deletion) the layer 3 switching table became corrupted and the wrong egress port was used for flows. This issue has been resolved.

PCR: 01254 Module: PRI Network affecting: No

When an M2 version of the AR020 PRI E1/T1 PIC was installed in a AR040 NSM it was not possible to select the T1 mode of operation regardless of the jumper setting. This issue has been resolved.

PCR: 01261 Module: IPG/VRRP Network affecting: No

A fatal error occurred when forwarding IP packets with VRRP enabled. This issue has been resolved.

PCR: 01265 Module: SWI Network affecting: No

When trunking was in operation, in some instances the switch transmitted tagged packets on untagged trunk ports. This issue has been resolved.

PCR: 01276 Module: SWI Network affecting: No

When the speed of one or more switch ports was forced to a half duplex setting and the ports were then added to a trunk group configured for full duplex operation, the port settings were not overridden by the trunk group speed setting. The trunk group speed setting will now take precedence over the port speed setting.

PCR: 01284 Module: PCI Network affecting: No

PAC cards with the Hifn 7951 chipset now operate correctly on Rapier switches. PAC cards with the older Hifn 7751 chipset are not supported on Rapier switches.

PCR: 01289 Module: VRRP Network affecting: No

The checksum in VRRP advertisements was not being calculated correctly. The calculation was not compatible with the RFC. This issue has been resolved.

PCR: 01290 Module: PPP Network affecting: No

When PPP was running over Ethernet to a client from another vendor, the Maximum Transmission Unit value for the link was not adjusted from the PPP default of 1500 to 1492. This issue has been resolved.

PCR: 01291 Module: IPG(IGMP) Network affecting: No

IGMP did not send the Start Up Query, and the Other Querier Present Timer did not change the Time Out value accordingly if Query Interval was changed. IGMP did not notify other registered parties (PIM and DVMRP) when a port was deleted from a membership group. IGMP reported a membership leave to other parties while it was still waiting for a reply to a group specific query from a leaving member. These issues have been resolved.

PCR: 02002 Module: OSPF Network affecting: No

The SHOW OSPF NEIGHBOUR command incorrectly displayed neighbour information. This issue has been resolved.

PCR: 02013 Module: SWI Network affecting: No

The switch was forwarding oversize packets. The maximum frame length was 1528 bytes. The maximum frame length is now 1524 bytes on gigabit ethernet ports and 1522 bytes on fast ethernet ports.

PCR: 02015 Module: SNMP Network affecting: No

A fatal error occurred when an invalid SNMP message was received. This issue has been resolved.

PCR: 02016 Module: SWI Network affecting: No

L3 filter commands now allow intermediate subnet masks.

PCR: 02023 Module: PIM Network affecting: No

PIM hello messages were not sent as tagged packets over a tagged port. This issue has been resolved.

PCR: 02028 Module: PPP Network affecting: No

When PPPoE AC received a PADT packet it caused a fatal error. This issue has been resolved.

PCR: 02030 Module: SWI Network affecting: No

Configuration and operation of L3 filters has been improved.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.